① NE-1045 ✓

(19)日本国特許庁（ＪＰ）　(12) 公表特許公報（Ａ）　(11)特許出願公表番号
特表2002－501700
（P2002－501700A）
(43)公表日　平成14年１月15日(2002.1.15)

| (51)Int.Cl.⁷ | 識別記号 | ＦＩ | テーマコード（参考） |
|---|---|---|---|
| Ｈ０４Ｌ　9/32 | | Ｇ０６Ｆ　15/00 | ３３０Ｆ |
| Ｇ０６Ｆ　15/00 | ３３０ | 17/60 | ２２２ |
| 17/60 | ２２２ | Ｈ０４Ｌ　9/00 | ６７５Ｂ |
| Ｈ０４Ｌ　9/08 | | | ６０１Ｆ |

審査請求　未請求　予備審査請求　有　（全 26 頁）

(21)出願番号　特願平10－548586
(86)（22)出願日　平成10年５月８日(1998.5.8)
(85)翻訳文提出日　平成11年11月５日(1999.11.5)
(86)国際出願番号　ＰＣＴ／ＵＳ９８／０９７７０
(87)国際公開番号　ＷＯ９８／５０８７５
(87)国際公開日　平成10年11月12日(1998.11.12)
(31)優先権主張番号　６０／０４６，０１２
(32)優先日　平成９年５月９日(1997.5.9)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　ジーティーイー　サイバートラスト　ソルーションズ　インコーポレイテッド
アメリカ合衆国　90017　カリフォルニア，ロサンジェルス，ウエスト　セブンス　ストリート　818
(71)出願人　ジーティーイー　サービス　コーポレイション
アメリカ合衆国　10011　ニューヨーク，ニューヨーク，サーティーンス　フロアー，エイス　アベニュー　111
(74)代理人　弁理士　倉内　基弘　（外１名）

最終頁に続く

(54)【発明の名称】　生物測定学的証明書

(57)【要約】
生物測定証明書が、生物測定証明書として、電子認証（証明）のために、デジタル証明書と組み合わされる。生物測定証明書は、生物測定証明書運用システムの使用を通して取り扱われる。生物測定証明書は、利害関係者の認証を要求するいかなる電子取引にも使用されることができるだろう。生物測定データは、生物測定入力装置を通して、登録されたユーザーの身体的特徴に対応したデータを受信することにより、生物測定証明書運用システムの生物測定データベースに予め記憶される。ネットワーク上で行われる以後の取引は、その時のユーザーの身体的特徴と電子取引から生成されるデジタル署名を持つ。電子取引は、デジタル署名のハッシュ値の再生されたハッシュ値との比較により正当性が証明される。ユーザーは、生物測定データベースに予め記憶されたユーザーの身体的特徴の生物測定証明書に対する比較により本人確認がなされる。

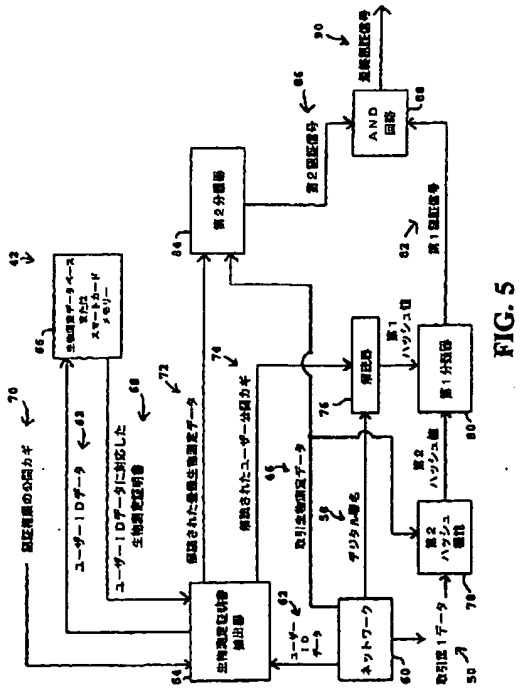

FIG. 5

【特許請求の範囲】

１．取引生物測定データ、取引第１データ、とそれらから生成されるデジタル署名を含む、ユーザーからの電子取引を認証（証明）することのための生物測定学的証明書システムであって：

取引第１データに含まれるユーザー登録名（ＩＤ）データに対応する生物測定証明書に応答し、そこから登録生物測定データとユーザー公開カギを抽出することのための、生物測定証明書抽出器；

登録生物測定データとユーザー公開カギに応答し、デジタル署名から第１ハッシュ値を取り戻すことのための、解読器；

取引生物測定データと取引第１データに応答し、そこから第２ハッシュ値を生成することのための、ハッシュ機能；と

第１ハッシュ値を第２ハッシュ値と比較することのためと、取引第１データと取引生物測定データの転送が正当であると確認するために第１認証信号を生成することのための、第１分類器、

とから成る、生物測定学的証明書システム。

２．生物測定証明書が、

登録生物測定データ；

ユーザー入力データ；

ユーザーの公開カギ；と

デジタル署名、

を含むシーケンスの形式である、請求項１に記載の生物測定学的証明書システム。

３．第１生物測定データを含むビットシーケンスの部分が約５００バイト長以上である、請求項２に記載の生物測定学的証明書システム。

４．第１分類器がデータマッチング処理を実行するためのプロセッサーを含む、請求項１に記載の生物測定学的証明書システム。

５．登録生物測定データと取引生物測定データとを比較することのためと、ユーザーが正当であることを証明するための第２認証信号を発生することのための、

第２分類器をさらに備える、請求項１に記載の生物測定学的証明書システム。

６．第２分類器が、生物測定データベースに記憶されている生物測定データの組により訓練された（認識できるように覚えさせられた）ニューロネットワークである、請求項１に記載の生物測定学的証明書システム。

７．取引生物測定データ、取引第１データと、それらから生成されるデジタル署名を含み、ユーザーを伴う電子取引の正当性を証明するための生物測定学的証明書システムであって：

ユーザーの身体的特徴の組に応答し、ユーザーの身体的状態に関係する、対応する取引生物測定データを生成する取引生物測定入力装置；

取引第１データと取引生物測定データに応答し、そこから第１ハッシュ値信号を生成することのための第１ハッシュ関数発生器；

ハッシュ値とユーザーの個人カギ信号からデジタル署名を生成するデジタル署名発生器、

を含む送信部分：と

ネットワークを通して、機能的に作用できるように送信部分と接続された受信部分であって、

取引第１データに含まれるユーザー登録名（ＩＤ）データに対応する生物測定証明書に応答し、そこから登録生物測定データとユーザー公開カギを抽出することのための生物測定証明抽出器；

登録生物測定データとユーザー公開カギに応答し、デジタル署名から第１ハッシュ値を取り戻すことのための解読器；

取引生物測定データと取引第１データに応答し、そこから第２ハッシュ値を生成することのための第２ハッシュ関数生成器；と

第１ハッシュ値を第２ハッシュ値と比較することのためと、取引第１データと取引生物測定データの転送が正当であることを証明するための第１認証信号を生成することのための第１分類器、

を含む受信部分、

から成る生物測定学的証明書システム。

８．取引生物測定入力装置が、対応する生物測定データを生成するためにユーザ

一の手相の画像を取り込む視覚の読み取り器である、請求項７に記載の生物測定学的証明書システム。

９．取引生物測定入力装置が、対応する生物測定データを生成するためにユーザーの虹彩の画像を取り込む視覚の読み取り器である、請求項７に記載の生物測定学的証明書システム。

１０．取引生物測定入力装置が、対応する生物測定データを生成するためにユーザーの網膜の画像を取り込む視覚の読み取り器である、請求項７に記載の生物測定学的証明書システム。

１１．取引生物測定入力装置が、対応する生物測定データを生成するためにユーザーの顔面の画像を取り込む視覚の読み取り器である、請求項７に記載の生物測定学的証明書システム。

１２．取引生物測定入力装置が、対応する生物測定データを生成するためにユーザーの身体の画像を取り込む視覚の読み取り器である、請求項７に記載の生物測定学的証明書システム。

１３．取引生物測定入力装置が、

ユーザーからの音声を受信する音声変換機；と

対応する生物測定データを生成するために、受信した音声をデジタル化する音声デジタイザー

を含む、請求項７に記載の生物測定学的証明書システム。

１４．第２分類器が、生物測定データベースに記憶されている生物測定データの組により訓練された（認識できるように覚えさせられた）ニューロネットワークである、請求項７に記載の生物測定学的証明書システム。

１５．第１と第２認証信号から、最終認証信号を生成することのための論理回路をさらに備える、請求項７に記載の生物測定学的証明書システム。

１６．第１ユーザーを伴う電子取引の正当性を証明することのための方法であって：

生物測定入力装置でユーザーの登録用の身体的特徴の組を受信すること；

登録用の身体的特徴の組に対応する登録生物測定データを生成すること；

登録生物測定データ、ユーザー入力データ、ユーザーの公開カギと、デジタル

署名から生物測定証明書を生成すること；と

メモリーに生物測定証明書を記憶すること；

の手段を含む、ユーザーを登録すること：

取引生物測定データ、取引第１データと、それらから生成されるデジタル署名を含む、ネットワーク上の電子取引を送信することであって、

その時のユーザーの身体的特徴の組を受信すること；

ユーザーの身体的状態に関係したその時の組から取引生物測定データを生成すること；

取引第１データと取引生物測定データから第１ハッシュ値信号を生成すること；

ハッシュ値とユーザーの個人カギ信号からデジタル署名を生成すること；

ネットワーク上でデジタル署名を送信すること；と

ネットワーク上で取引生物測定データと取引第１データを送信すること、

の手段を含む、電子取引を送信すること：

電子取引の正当性を証明する方法であって、

デジタル署名、取引生物測定データと、取引第１データをネットワークから受信すること；

取引第１データからユーザー登録名（ＩＤ）データを取り戻すこと；

メモリーからユーザーＩＤデータに対応した生物測定証明書を検索すること；

生物測定証明書から登録生物測定データとユーザー公開カギを抽出すること；

デジタル署名から第１ハッシュ値を取り戻すためユーザーの公開カギを使用して、デジタル署名を解読すること；

取引生物測定データと取引第１データから第２ハッシュ値を生成すること；

第１分類器を使用して、第１ハッシュ値を第２ハッシュ値と比較すること；

取引第１データと取引生物測定データの転送が正当であることを証明するために、第１認証信号を生成すること；

第２分類器を使用して、登録生物測定データと取引生物測定データを比較すること；と

ユーザーの正当性を証明するために、第２認証信号を生成すること、

の手段を含む、電子取引の正当性を証明すること、

の手段から成る、電子取引の正当性を証明することのための方法。

１７．正当性を証明することの手段が、第１と第２の認証信号の論理積（ＡＮＤ）をとることをさらに有する、請求項１６に記載の方法。

１８．ユーザーの身体的特徴の組を受信することの手段が、

登録生物測定入力装置として視覚の読み取り器を使用して、ユーザーの視覚的な特徴を受信すること、

の手段を含む、請求項１６に記載の方法。

１９．ユーザーの身体的特徴の組を受信することの手段が、

登録生物測定入力装置として音声デジタイザーを使用して、ユーザーの音声的な特徴を受信すること、

の手段を含む、請求項１６に記載の方法。

２０．登録生物測定データを生成することの手段が、登録生物測定データとして約５００バイト長以上のビットシーケンスを生成することの手段を含む、請求項１６に記載の方法。

【発明の詳細な説明】

# 生物測定学的証明書

## 発明の背景

１．発明の分野

この開示は、一般に、安全な通信に、そして特に、メッセージ(が正当な手続きにより発信されたものであるかどうか)を確認するための証明書の発行及び取り扱いに関する。

２．関連した技術の説明

近年、様々な処理に対するコンピューターネットワークと電気通信システムの使用は著しく増加している。買い物、購買、銀行業務、と投資サービス等の慣例的な取引は、コンピューターと電気通信の応用により新しい方向への成長を経験している。

慣例的な取引がこれまで典型的に人対人を基礎に行われているなかで、多くの電気通信を基礎にした通信が、遠隔でかつ視野に入らない（すなわち、電気通信を基礎にした当事者が決して会わない）で、行われている。

そのような電気通信を基礎にした取引とともに、インターネット上での購買、ホームバンキング、資金の電子転送、と電子仲介サービス等の、すべての種類の消費者に関わるサービス等を含む、電子サービスの遠隔のユーザーの信憑性を認識し、確認するための必要性が増加している。そのような電子取引はまた、例えば、極秘の記録、医療記録、課金記録、と企業記録のような極秘ではないが微妙なデータ等の、遠隔のリポジトリ（データベース）のデータのユーザーも含む。他の関連した、適当なまたは完全なセキュリティーを要求する領域は、契約等の電子書類の署名者の認証を含む。一般に、ローカルネットワークまたは公共のネットワーク上の、いかなる価値の電子サービスも、サービスの価値を守るために要求者の認証を要求する。さらに価値のあるサービスは、通常、さらに厳しい程度の認証を要求する。

歴史的に、電子サービスへのアクセスは、アカウントネーム等の識別技術と、個人識別番号（PIN:personal identification numbers）とパスワード等の認証

技術を通して与えられてきた。そのような認証技術は、PINとパスワードが簡単に予想されてしまうこと、記憶することが難しいこと、徹底的な自動サーチにより発見されやすいことにより、非常に安全であるとは認められていない。最近は、電子取引の認証のための第一候補として、デジタル証明書が持ち上がっている。

理想的には、X.509とANSI X.9スタンダードによって規定されるもの等の、デジタル証明書は、ユーザーまたは購買人と売人が、人対人の取引での公証人（Notary Public）による書類の認証に類似した方法で、電子書類と電子取引を認証することを可能にする。公開カギ暗号（publlc key cryptography）を含む暗号技術と、デジタル証明書の使用との組み合わせは、電子サービスの顧客に、より大きなレベルの信頼度をしみ込ませているオンライン電子取引のための、より大きな完全性、プライバシーと認証の程度を与えている。

例えば、従来技術でのそのような認証証明書は、図１に示されているように、メッセージと公開ガギをデータの組１０（それはシーケンスで、主体、すなわち、公開カギを持った個人または企業等の実体、に対応した主体固有ＩＤ１２を含んでもよい。）に連結することにより生成することができるだろう。図１に示されているように、データの組１０のフィールドは、バージョンナンバー、生成された証明書の順序に関する証明書のためのシリアルナンバー、発行者の名前、証明書の有効期限を決める有効期間、取引を送信しているユーザーまたは個人を識別する主体の名前、とアクセス特権等の特権と証明書の属性を示す他の拡張データを含むんでも良い。

ユーザーの主体固有ＩＤ１２は、例えば、取引を送信しているユーザーに関連した社会保証番号またはパスワードを示すMビットを含んでもよい。通常、以下の式のようになる。

M≒５０ビット≒６バイトまたはそれ以下

公開カギと取引データとの連結しているデータの組１０である認証証明書は、次に、ハッシュ値を生成するため、例えば、ワンウエイハッシュ関数（one-way hashing function）等のハッシュ関数を使用して、処理される。ハッシュ値は、

次に、署名される；すなわち、デジタル署名１４を生成するためにユーザーの個人カギ（private key）を使用し、暗号化される。デジタル署名１４は、次に、例えば、ネットワーク上の取引のための電子取引等の、認証証明書とメッセージに追加される。

上述したX.509とANSI X.9スタンダードは、それぞれのデータの組１０から固有のデジタル署名１４を生成するため、ハッシュ関数を組み込んでいる。そのようなワンウエイハッシュ関数は、取引データをハッシュ値から計算的に単独で得ることを実行不可能にすることができる。

デジタル証明書を組み込んだ認証証明書の従来技術での使用は、電子認証を利用している取引を改善するが、それはまだ、顧客等の人間の取引者を実際に認証することには達していない。それよりも、従来技術のそのようなデジタル証明書は、取引または署名に使われる個人暗号カギ（private cryptographic key）だけを認証する。個人カギはコンピューターと（／または）電子記憶装置に物理的に記憶されているので、そのような個人カギは個人カギに関連した実在とは物理的に関係しない。例えば、個人カギは、人のグループ、会社等の組織、または組織のグループであっても良く、それゆえ、個人カギは実際の人間に限定されない。

個人の識別のしるしは、以下の三つの大きなカテゴリーに分けられるだろう：個人の物理的な特徴に基づいてのしるし、すなわち、個人が何であるか；個人に知らされるパスワードのような、個人の知識に基づくしるし；と、割り当てられた情報に基づいたしるし、すなわち、識別される個人と、どのもう１つの個人が関係するか、または、識別される個人が関連する何を選ぶか。物理的なしるしを持った第一のカテゴリーは個人の生物測定学データに関係し、各個人に固有な（双子の同一な遺伝的構成の例外が知られているが）遺伝的構成、指紋、手相、虹彩と網膜の外観などのような、独特な特徴を含む。

知られてかつ（／または）割り当てられたしるしを持った、第２と第３のカテゴリーは、本人確認のために、社会保障番号、母の結婚前の名前、長距離電話用のカード番号のようなアクセス番号、と個人のパスワードのようなものを、記憶

することと公表することを個人が知りかつ（／または）責任を負う情報を含む。第２のカテゴリーはまた、本人確認のために、運転免許書とパスポートのようなものを携帯し、公表することを個人が負いかつ（／または）責任を負う。

個人カギは割り当てられたしるしである。したがって、個人カギを持った（人間の）取引者の身体的識別の不足は、そのような個人カギを使用する従来技術での本人確認技術の欠点である。多くの本人確認とセキュリティー技術は第２のカテゴリーの識別のしるしに依存しているので、従来技術での他の本人確認とセキュリティーは同様に欠点がある。

第１のカテゴリーの識別のしるしに基づく個人の本人確認のための技術が知られている；すなわち、物理的特徴による。例えば、フロム（Flom）らへの米国特許No. 4,641,349は、虹彩認識の実行システムを開示している。通常、そのような身体的特徴は各個人で固有なので、そのような身体的な特徴の識別技術は、身体的特徴の取り込みと正確な分類のために複雑な計算操作を要求する。したがって、そのような身体的特徴のための識別のしるしは、一般に、そのような識別のしるしの記憶と分類のために比較的膨大な量のメモリーを必要とする。

これまで、身体的特徴に基づいた本人確認技術の比較的膨大な量の計算の要求は、そのような本人確認技術の電子的取引での実行を妨げていた。

発明の要約

電子取引の本人確認での生物測定学的な識別と分類は、増大したセキュリティーと正確さを与えることがここで認識できる。

顧客の生物学的識別をデジタル証明書と組み合わせた、端から端までのセキュリティーメカニズムの実行をする生物測定学的証明書システムと方法がここで開示される。生物測定学的システムは、ユーザーを含む電子取引の正当性を証明し、ユーザーの身体的特徴の組に反応する生物測定入力装置を含み、ユーザーの身体的状態に関する、対応する第１生物測定データを生成する。

生物学的データは、生物測定入力装置を通して、登録したユーザーの身体的特徴に対応したデータを受信することにより、生物測定証明書処理システムの生物測定データベースに、生物測定証明書として、あらかじめ記憶される。その後の

、ネットワーク上で行われる取引は、取引第１データに追加される、その時点でのユーザーの身体的特徴から生成される取引生物測定データを持ち、それは次に、生物測定データベースに予め記憶されたユーザーの身体的特徴の生物測定データとの比較により、ユーザーの本人確認を行う。

図面の簡単な説明

開示された生物測定証明書システムと方法の特徴は、付随する図面と関連した、以下の本発明の好まれる具体例の詳細な説明を参照することにより、容易く明白になり、理解される。

図１は、従来技術の本人確認証明書を図解する。

図２は、開示された生物測定証明書システムと方法の生物測定証明書を図解する。

図３は、生物測定証明書登録装置を図解する。

図４は、電子取引の送信部分を図解する。

図５は、電子取引の受信と処理部分を図解する。

好まれる具体化の説明

図面への明確な詳細での参照で、図２に示されるように、同様または同一の要素、手順、特徴を同一とする共通の参照番号と共に、この開示は、主体固有ＩＤ１８と生物測定データ２０を含むデータの組１６から生物測定証明書を生成するための、生物測定証明書システムと方法を説明する。図２に示されるように、データの組１６を使用して生成されるデジタル署名２２は、生物測定証明書を形成するために生物測定証明書データの組１６に追加される。

開示された生物測定証明書システムは図３－５に示される。そこにおいて、図３には生物測定登録部分２４が示され、図４には送信部分４０が示され、図５には受信部分４２が示される。生物測定登録部分２４は、ユーザーに固有の生物測定証明書を生成するためユーザーの生物測定と関連した入力を処理し、その生物測定証明書は、生物測定データベースと（／または）スマートカードメモリー等のメモリーに記憶される。一度、そのような生物測定証明書が記憶されると、第

一ユーザーは、図４の送信部分４０から図５の受信部分４２へ送られる生物測定

的に安全化された電子取引を行うことができ、そこで、電子取引は正当であることが証明され、処理される。

図３への参照で、登録部分２４は、登録生物測定入力装置２６とユーザーデータ入力装置２８を含む入力装置の組を持つ。生物測定入力装置２６は、指紋、手相、虹彩と網膜の外観、声紋等の、ユーザーの身体的特徴から登録生物測定データを生成する。

登録生物測定入力装置２６は、指紋、手相、虹彩の外観、と網膜の外観を入力するために、映像のカメラと（／または）他の映像読み取り器を含むことができるだろう。例えば、アイデンティックス（IDENTIX）、富士通、とオーセンテック（AUTHENTEC）等の会社は、指紋を読み込むための、そのような装置を供給しているし、レコグニションシステムス（RECOGNITION SYSTEMS）は手相を読み込む装置を供給している。アイデンティファイ（EYE-DENTIFY）は、網膜画像装置を供給している会社の一例であり、アイリスキャン（IRISCAN）とセンサー（SENSAR）は虹彩画像装置を提供している会社の例である。

あるいは、登録生物測定入力装置２６は、ユーザーの音声の特徴を受信するために応用されてもよい。例えば、音声デジタイザーと関連してマイクが、音声を受信しデジタイズするために使用されても良い。ＢＢＮ、Ｔ－ＮＥＴＩＸ、とアルファテル（ALPHA-TEL）等の会社は、対応する生物測定データを生成するために、音声を受信しデジタイズするための、そのような装置を供給している。

この分野で知られている生物測定入力装置が、例えば、血液ランセット等の、遺伝物質の採集処理の手段によるユーザーの遺伝構成と同様に、カメラを通しての顔や身体の外観等の、他の身体的特徴を受信するために使用されても良い。

図２に示されている生物測定証明書は、登録機関３４の生物測定証明書生成器３２で、登録生物測定入力装置２６からの登録生物測定データの処理、ユーザーデータ入力装置２８からのユーザーＩＤ等のユーザー入力データの処理と、ユーザーの公開カギ３０の処理をすることで生成される。

そのような入力データは、記憶のためと、その後の、第１ユーザーと付随した第１ユーザーの電子取引の本人確認を行うための使用のためにメモリーに送られ

るデジタル生物測定証明書３８を生成するために、認証機関の個人カギ３６と共に処理される。

図２の生物測定証明書の中に取り込まれる登録生物測定データ２０は、生物測定入力装置２６を通して主体の身体的特徴から直接得られる。ユーザーの主体固有ＩＤ１８はMビットを含んでも良く、通常、M≒５０ビット≒６バイトまたはそれ以下である。一方、生物測定データ２０は通常、主体固有ＩＤ１８よりかなり大きなデータを含む。一般に、生物測定データ２０は、約５００ビット等のかなり大きいNビットを持つ。実際、生物測定データ２０の量は制限がなく；例えば、指紋は、指紋を一意的に区別する要所となる指紋外観を得るための、あるいは、指紋全体の画素を示すデータを得るためのいかなる解決のためにも視覚的にスキャンされても良い。したがって、生物測定データ２０は、２ＫＢまたは４ＭＢ等の、記憶するためのメモリー量を要求することもあるだろう。したがって、好まれる具体化では、NはMよりかなり大きい。

開示された生物測定証明書システムと方法の使用に先立って、例えば、個人が身元の証明を与えることを要求される登録処理を使用して、生物測定データベース６６が構築される；すなわち、出生証明書、運転免許書、現在の銀行口座データ、クレジットカードアカウントデータ、等の識別情報が登録機関に供給される。一度、登録機関がそのような証明で条件を満たすと、識別情報が登録システム２４の中に入れられ、図３に示されるように、それと同時に生物測定測定値が少なくとも１つの生物測定入力装置を使用して取り込まれる。

そのような記憶された生物測定測定値は、生物測定データベース６６に、上述の登録処理を行っている「予め登録された」個人に対応する、「予め記憶された」生物測定データを形成する。したがって、クロスオーバーエラー率の範囲で、予め登録された個人は、厳密に本人であることが確認され、登録されていない個人は拒絶される。

生物測定証明書３８は、次に、図５のメモリー６６に示されるように、生物測定データベースまたはスマートカードのメモリー等のメモリーに記憶されるために送られる。ユーザーの対応する生物測定証明書が直接にかつ安全にネットワークの中心生物測定データベースまたはユーザーのスマートカードの個人メモリー

等のメモリー６６に記憶されるように、図３の登録システム２４は、ネットワークに結合した中心登録ステーションに置かれる。したがって、メモリー６６としての中心生物測定データベースは、インターネットまたは他のネットワーク上で電子商業等の取引を行っているユーザーのネットワークに供給することができるだろう。あるいは、キオスクと端末とＡＴＭ等の他の装置がメモリー６６にアクセスし、第１ユーザーの安全化された生物測定証明書を得ることができるように、メモリー６６を持っている第１ユーザーのスマートカードは、生物測定証明書を予め記憶することができるだろう。

図４－５への参照で、電子取引を行うために、第１ユーザーは図４の取引システム４０を使用する。第１ユーザーは、第１ユーザーと関連したその時点での生物測定としての取引生物測定データ４６を生成するために、取引生物測定入力装置４４を使用する。第１ユーザーはまた、取引データ入力装置４８を通して、取引第１データ５０を生成する。例えば、取引第１データ５０は、インターネット上の購買される製品の選択を含んでも良いし、またはＡＴＭを通しての電子資金転送を含んでも良い。取引第１データ５０はまた、第１ユーザーを識別し、第１ユーザーと取引第１データの残りの部分とを関連させる、ユーザーＩＤデータを含んでも良い。

図５に示されているように、取引生物測定データ４６と取引第１データ５０の両者は、取引受信部分４２に受信されるために、ネットワーク６０上を変更されずに明文で送られても良いし、または選択的に、この分野で知られている付加的な暗号技術で暗号化されて送られても良い。

さらに、図４の取引送信部分４０で、取引生物測定データ４６と取引第１データ５０の両者は、第１ハッシュ値を生成するために、例えば、ワンウエイハッシュ関数等の、第１ハッシュ機能（関数）５２を使用して処理される。ＲＳＡとＳＨＡ－１は、暗号化とハッシュ関数のために使われる公開カギ暗号方法とワンウエイハッシュ法の例である。ＲＳＡ法は、例えば、リベスト（Rivest）らへの米国特許No. 4,405,829に記述されており、ここでも参照として取り入れられている。ＳＨＡ－１法は、例えば、チルド（Childs）らへの米国特許No. 5,623,545に記述されており、ここでも参照されている。

第１ハッシュ値は、次に、デジタル署名機能５４に送られ、そこにおいて、ハッシュ値は署名される；すなわち、第１ハッシュ値を組み込みながら、デジタル署名５８を生成するために第１ユーザーの個人カギ５６を使用して暗号化される。デジタル署名５８は、次に、ネットワーク６０へ送られる。

取引生物測定データ４６、取引第１データ５０、とデジタル署名５８を構成する取引データの組は、セパレートビットストリームと（／または）データパケットとして送られても良いし、または、データシーケンスのビット単位の加算のための加算器等の連結器を使用して関連したデータシーケンスを追加することにより、一緒に送られても良い。さらに、ソフトウエアがそのようなデータを追加するために使用されても良い。データ４６、５０、と５８は、電話回線、衛星通信、と（／または）インターネットを含んでも良いネットワーク６０へ送られる。

図５への参照で、ネットワーク６０からの電子取引を受信したあと、受信部分４２は、取引第１データ５０からのユーザーＩＤデータ６２を、生物測定証明書抽出器６４へ送る。生物測定証明書抽出器６４は、生物測定データベースやスマートカードメモリー等のメモリー６６に記憶された、対応する生物測定証明書をアクセスするために、ユーザーＩＤデータ６２を使用する。すなわち、第１ユーザーが、図３に示される登録システム２４を使用して第１ユーザーの生物測定的特徴から生成される、対応する生物測定証明書を以前に格納している場合、第１ユーザの生物測定証明書が、社会保障番号等の第１ユーザーのユーザーＩＤに応じて検索されるだろう。

メモリー６６はユーザーＩＤデータ６２を受信しても良いし、または、第１ユーザーのユーザーＩＤデータ６２に対応するいかなる生物測定証明書を検索するために、生物測定証明書抽出器６４からの命令を受信しても良い。有効なものがない場合、受信部分４２は、例えば、有効な生物測定証明書がないことを示すために、生物測定証明書抽出器６４に拒絶信号を生成しても良い。

したがって、電子取引の本人確認を要求しているが、登録（すなわち、メモリー６６に予め記憶された、対応する生物測定証明書を持つこと）に失敗したいかなるユーザーも、正当であるとは認められない。受信部分４２は、対応する非本人確認のメッセージを生成しても良いし、取引に本人確認がないことを示すため

に、ネットワーク６０を通して送信部分４０にそのようなメッセージを送っても良い。

一方、対応したユーザーＩＤデータを持った第１ユーザーに対応する生物測定証明書が有効である場合、生物測定証明書６８は検索され、認証機関の公開カギ７０を使用して生物測定証明書６８を解読するために生物測定証明書抽出器６４へ送られる。よって、生物測定証明書抽出器６４は第１ユーザーに関連した解読された登録生物測定データ７２と解読されたユーザー公開カギ７４を得る。

解読された公開カギ７４は、次に、送信部分２４からネットワーク６０を通して送られたデジタル署名を解読するために、解読器へ送られる。解読器７６は、次に、第１ハッシュ機能（関数）５２によってデジタル証明書５８の中に組み込まれた第１ハッシュ値を抽出する。

受信部分２４は、送信部分２４の第１ハッシュ機能（関数）５２と同一の第２ハッシュ機能（関数）７８を使用して第１ハッシュ値を再生することを試みることにより、第１ハッシュ値が正当であることを確認する。第２ハッシュ機能（関数）７８は、送信部分２４から明文で、または選択的にこの分野で知られている付加的な暗号技術で暗号化されて送信された取引生物測定データ４６と取引第１データ５０を、ネットワーク６０から受信する。第２ハッシュ機能（関数）７８は、よって、第１ハッシュ機能（関数）５２に適用されたのと同じ入力データから第２ハッシュ値を生成する。

第１と第２のハッシュ値は、次に、第１と第２のハッシュ値の間の照合を決めるために比較器やソフトウエアの照合ルーチン等の第１分類器８０によって比較される。第１照合信号８２は、独立に生成された両方のハッシュ値がマッチするかどうかを示すために生成される。

したがって、両者がマッチした場合、受信部分４２は、取引生物測定データ４６と取引第１データ５０の両方が、その組み合わせで、本物であり、ネットワーク６０上の転送中に変更がなされていないことを決定する。

さらに、受信部分４２は、電子取引が本当に、取引生物測定データ４６に対応した、指示されたユーザーからでるかを決定する；すなわち、取引生物測定データ４６が確実でないかも知れないことや、あるいは、解読されたユーザーの公開

カギ７４が、特定の会社の従業員等の特定のグループに普通に分けられている公開カギであるだろうことである。

したがって、受信部分４２は、取引生物測定データ４６として取引中に生成される第１ユーザーの生物測定データを、登録システム２４を使用して登録処理中に第１ユーザーから以前のデータとして生成された登録生物測定データと比較する。解読された登録生物測定データ７２となる生物測定証明書抽出器６４により解読された登録生物測定データは、ネットワーク上を明文、または選択的にこの分野で知られる付加的な暗号技術により暗号化されて送られた取引生物測定データ４６と比較されるために第２分類器８４へ適用される。

第２分類器８４は、決定値を得るための、生物測定データの比較のための、比較器、またはデータ照合を行うソフトウエアルーチンか他のハードウエア／ソフトウエア装置となるだろう。あるいは、第２分類器８４は、エラーの許容範囲内で生物測定入力装置を使用して得られた生物測定データ４６、７２の組が同じ個人から得られたものかどうかを分類（判定）するための、訓練された（認識できるように覚えさせられた）ニューロネットワークと（／または）ファジー論理分類器であっても良い。（ニューロネットワークを使用した画像及びデータシーケンスの本人確認のための、）そのような分類方法は、エクレス（Eccles）への米国特許No. 5,619,620に記述されており、ここでも参照として取り込まれている。

第２分類器８４は、電予取引を送信しているユーザーの本人確認の照合を示す、ＹＥＳかＮＯまたは正か誤に対応する論理値等の、第２照合信号８６の形式で決定を生成する。あるいは、照合決定は、例えば、本人確認の確実性のパーセンテージに対応する数値となっても良いだろう。第２分類器８６は、例えば、９８％の本人確認等の、電子取引の処理を進行させるために超えることになっている、予め決められた閾値を含んでも良いだろう。

図５に示されている受信部分４２は、オンライン購買や電子資金転送等の、取引第１データを処理するために、照合信号８２、８６に応答する。したがって、取引処理システム（図示せず）もまた、受信部分４２に含むことができるだろう。あるいは、図５の受信部分４２は、外部の取引処理システムに接続されても良い。

もう１つの代替の具体化で、受信部分は、照合信号８２、８６から最終照合信号９０を生成するために、論理ＡＮＤゲートや他の論理メカニズム等の、図５に示されるＡＮＤ回路を含むこともできるだろう。したがって、分類器８０、８４の両者が、取引第１データ５０と同様に取引生物測定データ４６がネットワーク上を十分安全に送信されたと決定した場合だけ、すべての取引の安全性を反映する最終照合信号９０が生成される。

第１分類器８０は完全な分類器であるのに対し（すなわち、ハッシュ値の完全な照合だけが本人確認を生成するが）、第２分類器８４は、第２分類器のエラーの許容と（／または）生物測定に関連するクロスオーバーエラー率を反映するために、相対的な本人確認と（／または）本人確認の等級上に等級付けられた数値を反映しているパーセンテージを生成しても良い。したがって、ファジー論理の適用が、第２照合信号８６としての取引生物測定データ４６の本人確認の明瞭な決定を生成するために使用されても良い。

生物測定証明書を使用するとき、識別と本人確認のためのクロスオーバーエラー率は約２．０％以下で、０．５％以下であってもよいだろう。この分野で知られている、さらに進んだ生物測定入力装置２６、４４と分類器８０、８４の適用により、地球上のいかなる個人への実質的に完全な本人確認をも得ることができるだろう。

開示された生物測定証明書システムと方法は、１９９６年１２月２０日に提出された、本出願人による米国特許出願No.08/770,824（タイトル「VIRTUAL CERTIFICATE AUTHORITY」）に記述されているネットワークを含むこともでき、ここでも参照として取り入れられている。そのようなシステムは、生物測定証明書を形成するために、ユーザーの生物測定データを識別情報に暗号法で組み合わせるために、ここで記述されている生物測定証明書の使用を含むために適合することができるだろう。公開カギ技術の使用は、取引／署名の本人確認処理が、取引の必要に依って、中央または遠隔の両方でなされることを可能にする。

開示された生物測定証明書システムと方法が、好まれる具体化への参照とともにここで詳細に示され、記述されたきたが、本発明の範囲及び意図から外れることなく、多様な形式及ぶ詳細での変更がなされることは理解できる。したがって

、ここで提案されたようないかなる変更も制限されず、本発明の範囲に入るとみなされる。

【図１】

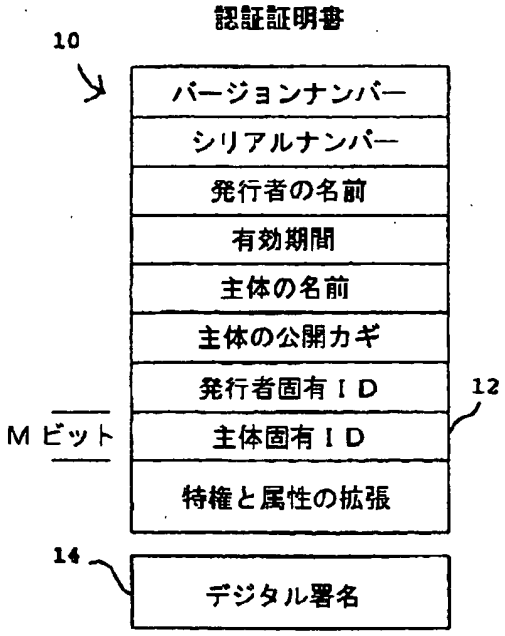


**FIG. 1**
（従来の技術）

【図２】

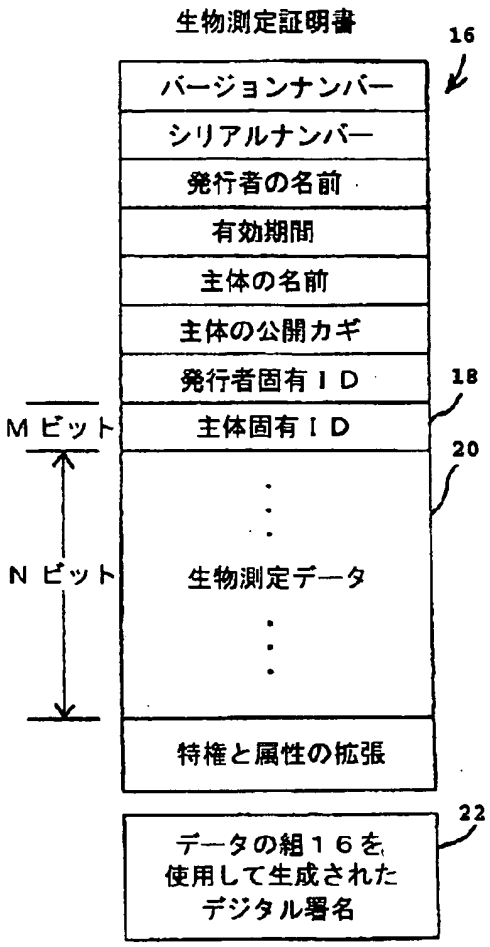
生物測定証明書
16
バージョンナンバー
シリアルナンバー
発行者の名前
有効期間
主体の名前
主体の公開カギ
発行者固有ＩＤ
18
Ｍビット
主体固有ＩＤ
20
Ｎビット
生物測定データ
特権と属性の拡張
22
データの組１６を
使用して生成された
デジタル署名

FIG. 2

【図３】

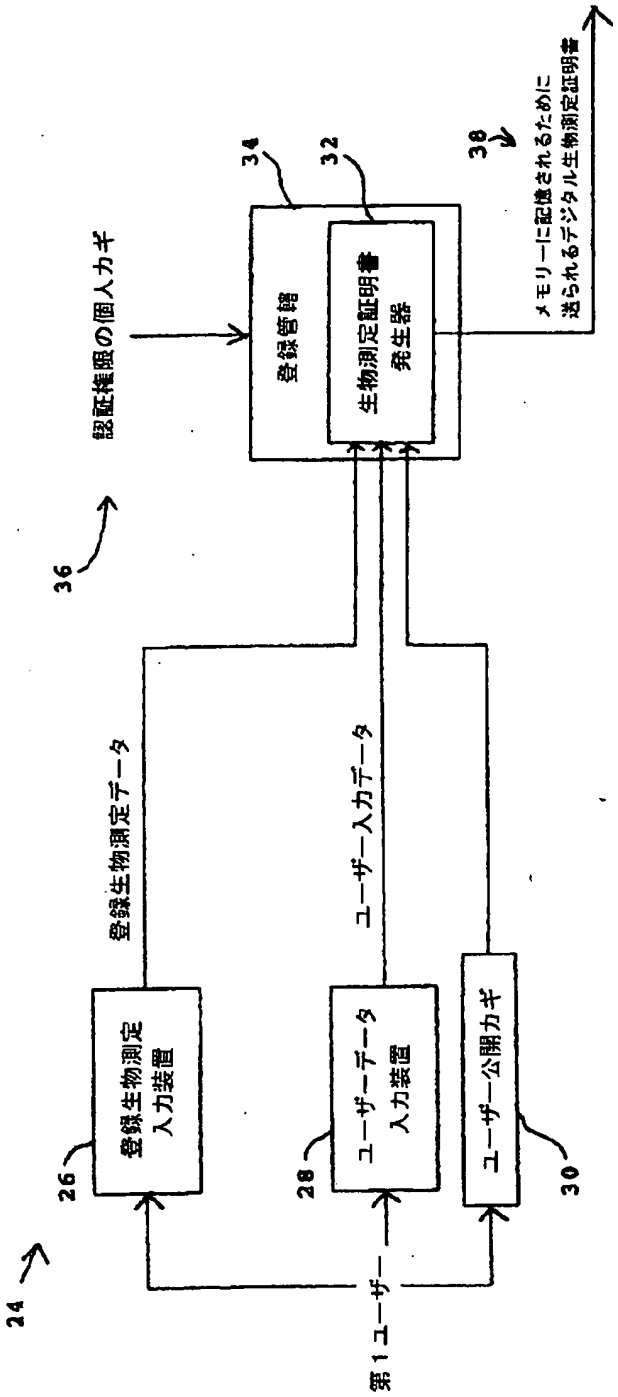
認証権限の個人カギ
登録管轄
生物測定証明書発生器
メモリーに記憶されるために送られるデジタル生物測定証明書
登録生物測定データ
ユーザー入力データ
登録生物測定入力装置
ユーザーデータ入力装置
ユーザー公開カギ
第１ユーザー
24
26
28
30
32
34
36
38

FIG. 3

【図４】

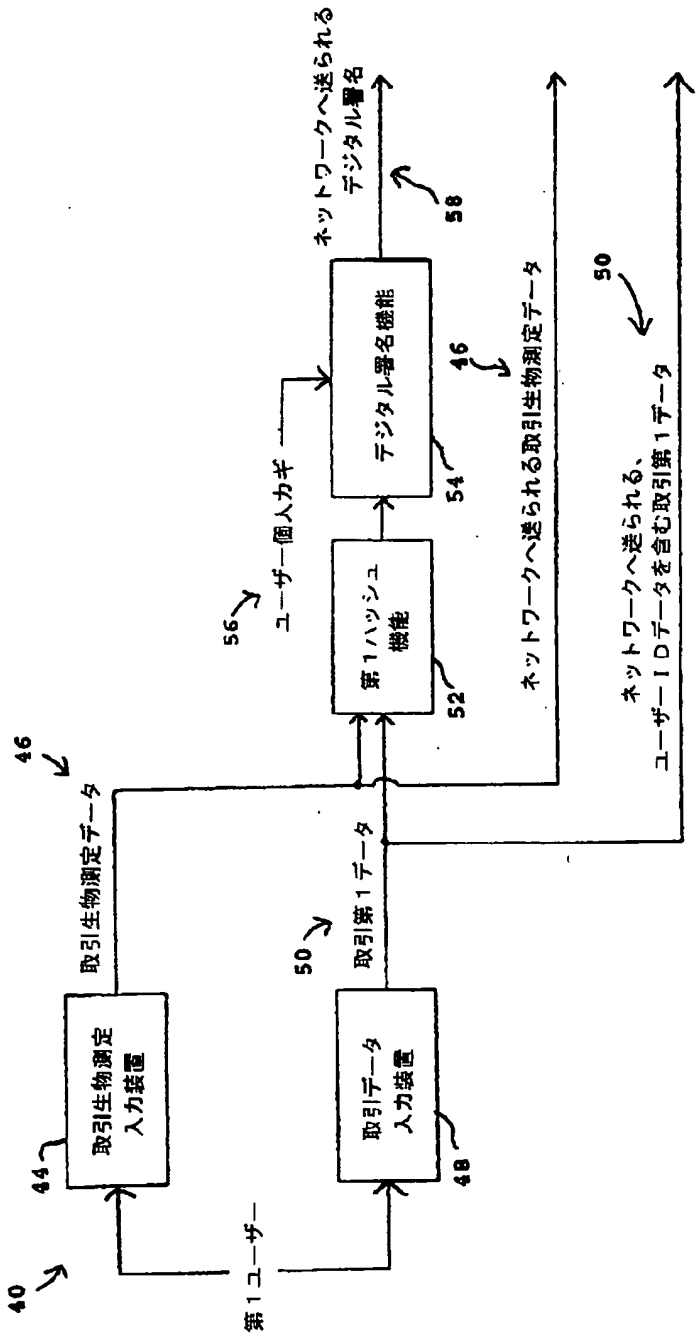
40
第１ユーザー
44
取引生物測定
入力装置
48
取引データ
入力装置
46
取引生物測定データ
50
取引第１データ
56
ユーザー個人カギ
52
第１ハッシュ
機能
54
デジタル署名機能
58
ネットワークへ送られる
デジタル署名
46
ネットワークへ送られる取引生物測定データ
50
ネットワークへ送られる、
ユーザーＩＤデータを含む取引第１データ

FIG. 4

【図５】

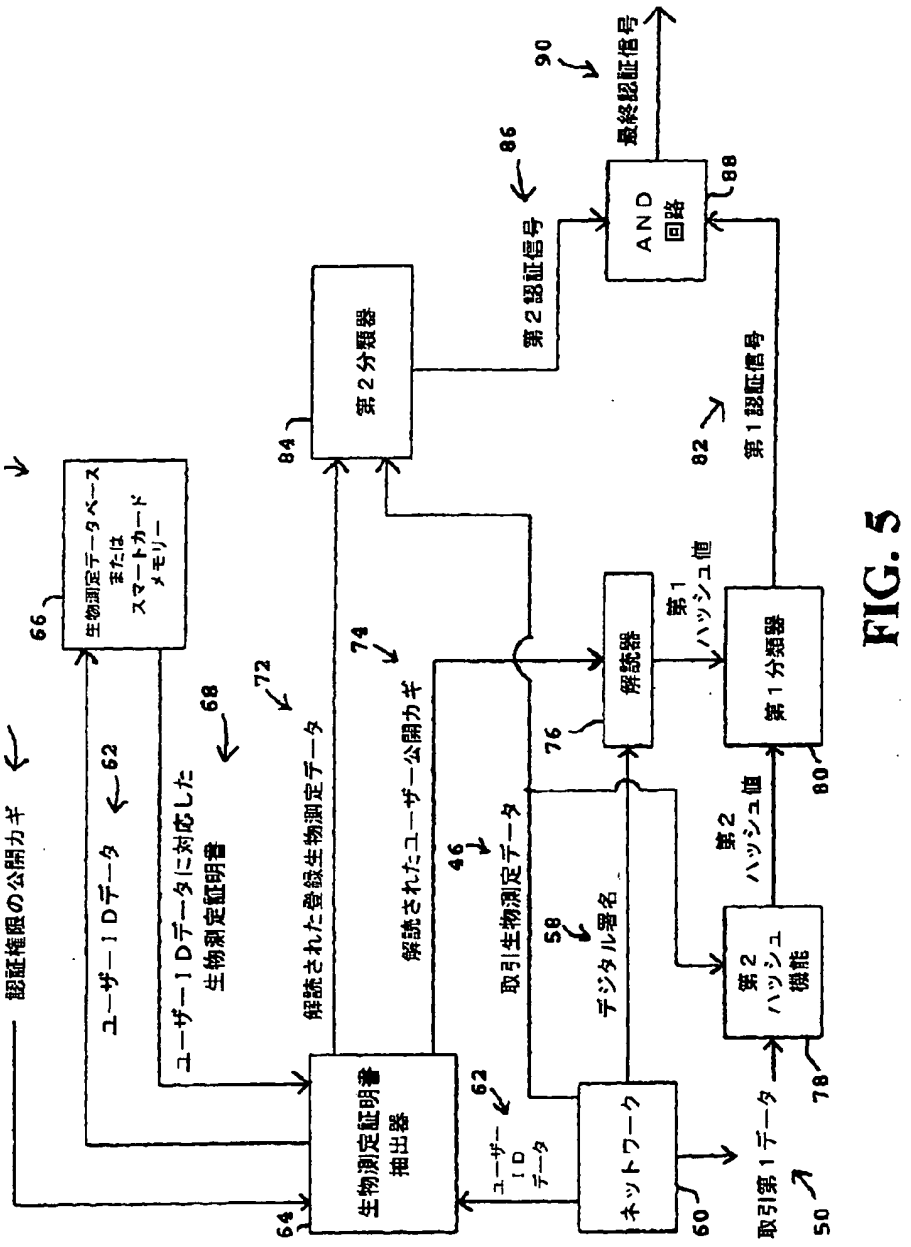
認証権限の公開カギ
70
ユーザー１Ｄデータ
62
ユーザー１Ｄデータに対応した
生物測定証明書
68
解読された登録生物測定データ
72
解読されたユーザー公開カギ
74
取引生物測定データ
46
デジタル署名
58
ユーザー
１Ｄ
データ
62
生物測定証明書
抽出器
64
ネットワーク
60
取引第１データ
50
生物測定データベース
または
スマートカード
メモリー
42
66
第２分類器
84
解読器
76
第１
ハッシュ値
第１分類器
80
第２
ハッシュ値
第２
ハッシュ
機能
78
第２認証信号
86
第１認証信号
82
AND
回路
88
最終認証信号
90

FIG. 5

【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/09770

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :G06K 9/20; H04K 1/00; H04L 9/28, 9/00
US CL :Please See Extra Sheet.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
U.S. : 382/115, 116-118, 124, 155, 190; 395/21; 380/2, 9, 23-25, 28, 46; 178/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
APS: BIOMETRIC, FINGERPRINT, IRIS, EYE, SPEECHM, VOICE, HASH, ENCRYPT, DECRYPT, NEURAL, EXTRACT, CLASS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | US 4,868,877 A (FISCHER) 19 SEPTEMBER 1989, see Abstract, col. 10, and figs. 1-4 | 1, 7, 16 |
| Y | US 4,405,829 A (RIVEST et al.) 20 SEPTEMBER 1983, see Abtract, col. 1-6, and fig. 7 | 1, 7, 16 |
| Y | US 5,623,545 A (CHILDS et al.) 22 APRIL 1997 see Abstract, col. 1-6, and figs. 1-11 | 1, 7, 16 |
| Y | US 4,641,349 A (FLOM et al.) 03 FEBRUARY 1987, see Abstract, col. 1-13, and figs. 2-7 | 1-20 |
| Y | US 5,263,097 A (KATZ et al.) 16 NOVEMBER 1993, see Abstract, col. 1-9, and fig. 3-7 | 1-20 |

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

| | | | |
|---|---|---|---|
| * | Special categories of cited documents: | "T" | later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention |
| "A" | document defining the general state of the art which is not considered to be of particular relevance | "X" | document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone |
| "E" | earlier document published on or after the international filing date | "Y" | document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| "L" | document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | "&" | document member of the same patent family |
| "O" | document referring to an oral disclosure, use, exhibition or other means | | |
| "P" | document published prior to the international filing date but later than the priority date claimed | | |

| | |
|---|---|
| Date of the actual completion of the international search<br>25 SEPTEMBER 1998 | Date of mailing of the international search report<br>29 OCT 1998 |
| Name and mailing address of the ISA/US<br>Commissioner of Patents and Trademarks<br>Box PCT<br>Washington, D.C. 20231<br>Facsimile No. (703) 305-3230 | Authorized officer<br>JOSE L. COUSO<br>Telephone No. (703) 305-3800 |

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/09770

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

382/115, 116-118, 124, 155, 190.; 395/21; 380/2, 9, 23-25, 28, 46; 178/22

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW

(72)発明者 デュルード，ロバート
アメリカ合衆国 02181 マサチューセッツ，ウエルズリー，ラファイエット サークル 14
(72)発明者 マスグレイブ，クライド
アメリカ合衆国 75035 テキサス，フリスコ，フェアフィールド プレイス 3620